Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method to protect a file system from a viral infection, comprising:
flagging a program in response to at least one of:
opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file;
the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system;
the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and
the program attempting to write or append a remote file to the local file system.

[c2] 2. The method of claim 1, further comprising inhibiting a write or append operation associated with program in response to flagging the program.

[c3] 3. The method of claim 1, further comprising monitoring all file operations associated with the program in response to the program not being in a safe list.

[c4] 4. The method of claim 1, further comprising permitting selected read and write operations in response to a predefined rules table.

[c5] 5. The method of claim 1, further comprising sending an alert in response to flagging the program.

[c6] 6. The method of claim 1, further comprising storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program.

[c7] 7. The method of claim 1, further comprising sending an alert to a network monitoring system in response to flagging the program.

[c8] 8. The method of claim 1, further comprising logging any file system operations including recording a filename and a location where the local or shared file is written.

[c9] 9. A method to protect a file system from a viral infection, comprising:
monitoring predetermined file system operations associated with a program; and

logging any predetermined file system operations associated with the program including recording a filename and a location where a file is written.

[c10] 10. The method of claim 9, further comprising selecting the program for monitoring in response to the program not being on a safe list.

[c11] 11. The method of claim 10, further comprising logging any file system operations associated with any programs on the safe list.

[c12] 12. The method of claim 9, further comprising receiving a notification that the program intends to perform one of the predetermined file system operations.

[c13] 13. The method of claim 9, further comprising following a predefined procedure in response to a level of security set.

[c14] 14. The method of claim 9, further comprising flagging the program in response to the program attempting to perform one of the predetermined file system operations.

[c15] 15. The method of claim 14, further comprising flagging the program in response to at least one of:
the program opening a local file on a local file system to

perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file;

the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system;

the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and

the program attempting to write or append a remote file to the local file system.

[c16] 16. The method of claim 14, further comprising inhibiting any predetermined file system operations associated with the program in response to the program being flagged.

[c17] 17. The method of claim 9, further comprising sending an alert in response to the program attempting to perform any predetermined file system operations.

[c18] 18. The method of claim 17, further comprising sending the alert to a network monitoring system.

[c19] 19. The method of claim 9, further comprising presenting an alert to a user for approval before the predetermined file system operation is performed by the program.

[c20] 20. The method of claim 9, further comprising requiring approval before performing any predetermined file system operations associated the program in response to the program not being on a safe list.

[c21] 21. A system to protect a file system from a viral infection, comprising:
a file system protection program including:
means to monitor predetermined file system operations associated with another program, and
means to log any predetermined file system operations associated with the other program including recording a filename and a location where a file is written.

[c22] 22. The system of claim 21, further comprising a safe list, wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list.

[c23] 23. The system of claim 21, further comprising a log to record any predetermined file system operations.

[c24] 24. The system of claim 21, further comprising means to

flag the other program in response to at least one of:
the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file;
the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system;
the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and
the other program attempting to write or append a remote file to the local file system.

[c25] 25. The system of claim 21, further comprising means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations.

[c26] 26. The system of claim 25, further comprising means to send an alert in response to flagging the other program.

[c27] 27. The system of claim 25, further comprising:
a network monitoring system; and

means to send an alert to the network monitoring system in response to flagging the other program.

[c28] 28. The system of claim 25, further comprising means to inhibit predetermined file system operations associated with the other program in response to the program other being flagged.

[c29] 29. The system of claim 25, further comprising:
means to present an alert to a user; and
means for the user to approve the one of the predetermined file system operations before being performed by the other program.

[c30] 30. A method of making system to protect a file system from a viral infection, comprising:
providing a file system protection program including:
providing means to monitor predetermined file system operations associated with another program, and
providing means to log any predetermined file system operations associated with the other program including recording a filename and a location where a file is written.

[c31] 31. The method of claim 30, further comprising:
providing a safe list; and
adapting the file system protection program to monitor

the other program in response to the other program not being on the safe list.

[c32] 32. The method of claim 30, further comprising forming a log to record any predetermined file system operations.

[c33] 33. The method of claim 30, further comprising providing means to flag the other program in response to at least one of:
the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file;
the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system;
the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and
the other program attempting to write or append a remote file to the local file system.

[c34] 34. The method of claim 30, further comprising provid-

ing means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations.

[c35] 35. The method of claim 34, further comprising providing means to send an alert in response to flagging the other program.

[c36] 36. The method of claim 34, further comprising:
providing a network monitoring system; and
providing means to send an alert to the network monitoring system in response to flagging the other program.

[c37] 37. The method of claim 34, further comprising:
providing means to present an alert to a user; and
providing means for the user to approve the one of the predetermined file system operations before being performed by the other program.

[c38] 38. A computer-readable medium having computer-executable instructions for performing a method, comprising:
monitoring predetermined file system operations associated with a program; and
logging any predetermined file system operations associated with the program including recording a filename and a location where a file is written.

[c39] 39. The computer-readable medium having computer executable instructions for performing the method of claim 38, further comprising selecting the program for monitoring in response to the program not being on a safe list.

[c40] 40. The computer-readable medium having computer executable instructions for performing the method of claim 38, further comprising following a predefined procedure in response to a level of security set.

[c41] 41. The computer-readable medium having computer executable instructions for performing the method of claim 38, further comprising flagging the program in response to the program attempting to perform one of the predetermined file system operations.

[c42] 42. The computer-readable medium having computer executable instructions for performing the method of claim 41,further comprising flagging the program in response to at least one of:
the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file;
the program reading or opening itself and the program

attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system;

the program attempting to write or append the local file to the shared or network file system and preserve a file-name of the local file in the shared or network file system; and

the program attempting to write or append a remote file to the local file system.

[c43] 43. The computer-readable medium having computer executable instructions for performing the method of claim 41, further comprising inhibiting any predetermined file system operations associated with the program in response to the program being flagged.

[c44] 44. The computer-readable medium having computer executable instructions for performing the method of claim 38, further comprising sending an alert in response to the program attempting to perform any predetermined file system operations.